REMARKS:

Claims 35 and 37 are pending in this application.

Claims 35 and 37 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Reconsideration is respectfully requested.

The Office Action contends that the method as recited in claim 35 is broad enough to read on a method where the register lacks sufficient funds and the steps of sending, receiving, deducting and activating to not take place, and concludes from this that the claims fail to particularly point out and distinctly claim the subject matter regarded as the invention. Applicants respectfully disagree.

The primary purpose of the requirement of definiteness of claim language is to ensure that the scope of the claims is clear so the public is informed of the boundaries of what constitutes infringement of the patent. In reviewing a claim for compliance with 35 U.S.C. 112, second paragraph, the examiner must consider the claim as a whole to determine whether the claim apprises one of ordinary skill in the art of its scope and, therefore, serves the notice function required by 35 U.S.C. 112, second paragraph, by providing clear warning to others as to what constitutes infringement of the patent. See, e.g., *Solomon v. Kimberly-Clark Corp.*, 216 F.3d 1372, 1379, 55 USPQ2d 1279, 1283 (Fed. Cir. 2000). If the language of the claim is such that a person of ordinary skill in the art could not interpret the metes and bounds of the claim so as to understand how to avoid infringement, a rejection of the claim under 35 U.S.C. 112, second paragraph, would be appropriate. See *Morton Int'l, Inc. v. Cardinal Chem. Co.*, 5 F.3d 1464, 1470, 28 USPQ2d 1190, 1195 (Fed. Cir. 1993). Applicants respectfully submit that the claims clearly apprise one of ordinary skill in the art of its scope and that the metes and bounds of the claims are easily interpreted so as to understand how to avoid infringement. The Office Action is attempting to improperly read unclaimed limitations into the claim. The scope of the claims is clear as to what constitutes infringement of the claims. The claims do not read on how the method is to perform if the register lacks sufficient funds, nor do they need to. The scope of the

claim is directed to the steps performed if the register does contain sufficient funds. As stated in the MPEP, section 2173.04, if the scope of the subject matter embraced by the claims is clear, and if applicants have not otherwise indicated that they intend the invention to be of a scope different from that defined in the claims, then the claims comply with 35 U.S.C. 112, second paragraph.

Applicants respectfully submit that the claims are not indefinite as stated above and are in full compliance with 35 U.S.C. 112.

Claims 35 and 37 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Fisher (U.S. Patent No. 5,005,200) in view of Taylor (U.S. Patent No. 5,530,232). Reconsideration is respectfully requested.

Applicants' invention relates to a secure user certification system for electronic commerce that provides an accounting system for services provided. In electronic commerce, various parties conduct activities without face to face contact. As such, it is desirable for each party to any transaction to be able to determine and verify the authenticity of the other party to the transaction, as well as ensure sufficient security for any commerce conducted electronically. Such security services could include, for example, message integrity, message authentication, message confidentiality, and message non-repudiation. In an electronic commerce environment these security services are achieved by cryptographic techniques such as digital signature, hash codes, encryption algorithms, and the like. To effectively implement the above, a party to an electronic commerce transaction requires access to a secure cryptographic device capable of securely implementing these cryptographic techniques. According to the present invention, a certificate meter provides certificate management services including use of cryptographically secured certificates. Payment for the processing and issuing, by the certificate authority, of the electronic certificates can be made using funds stored in the meter. Thus, the present invention provides a party to an electronic commerce transaction access to a secure cryptographic device, i.e., a certificate meter, associated with a certificate authority, while providing the certificate authority with a convenient payment system to allow the certificate authority to get paid for processing and issuing of the electronic certificates.

As illustrated in Fig. 5 of the present specification, after the certificate meter receives a request for a cryptographic certificate at 502, it is determined on 504 if sufficient funds are available in the register to obtain the certificate. If sufficient funds are available, then at 510 the certificate meter securely generates a public and private key pair. The private key is, therefore, never available outside of the secure housing of the postage and certificate meter subsystem 218. In a preferred embodiment the private key is not known to anyone, including the certificate owner, therefore the postage and certificate meter can enforce charges for any use of the private key. At step 512, the certificate meter sends a request to a certificate authority to generate a certificate including the public key of the public/private key pair generated at step 510. After the certificate has been received from the certificate authority, at step 520, funds are deducted from the register of the certificate meter for the generation of the requested certificate, which activates the user's private key. The private key can now be used to sign messages, and the signed message, along with the certificate, can be sent to a third party. The third party can use the public key contained within the certificate to verify the authenticity of the message.

In view of the above, claim 35 as is directed to a method for obtaining a cryptographic certificate that comprises "receiving at a metering device a request for a cryptographic certificate, the metering device including a register having funds stored therein; determining if sufficient funds are present in the register for obtaining the certificate; if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key; sending a certificate request to a certificate authority, the certificate request including the public key of the cryptographic key pair; receiving a cryptographic certificate from the certificate authority, the cryptographic certificate including the public key of the cryptographic key pair generated by the metering device; deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair."

Fischer, in contrast, is directed to a public key cryptographic system with enhanced digital signature certification that authenticates the identity of the public key holder. Specifically, in Fischer, a trusted authority creates a digital message which contains the claimant's public key

and the name of the claimant and a representative of the authority signs the digital message with the authority's own digital signature. This digital message, often referred to as a certificate, is sent along with the use of the claimant's own digital signature. Any recipient of the claimant's message can trust the signature, provided that the recipient recognizes the authority's public key. (Col. 3, lines 53-64). The system of Fischer provides the ability to specify a variety of attributes associated with the certification, such as specifying the authority or constraints which are conferred on the certifee by the certifier. (Col. 4, lines 56-62).

Thus, while Fischer discloses the use of certificates for providing security functions, there is no disclosure, teaching or suggestion in Fischer of "receiving at a metering device a request for a cryptographic certificate, the metering device including a register having funds stored therein, determining if sufficient funds are present in the register for obtaining the certificate, if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key" as is recited in claim 35. There is also no disclosure, teaching or suggestion in Fischer of "deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair" as is recited in claim 35. In Fisher, the public and private keys are generated and activated at the same time. Claim 35, in contrast, specifically recites that the key pair is generated if there are sufficient funds present in the register, but the private key of the key pair is not activated until after the funds have been deducted from the register.

To overcome some of the above deficiencies the Office Action relies on the reference to Taylor. Taylor is directed to a multi-application data card capable of substituting for a plurality of existing single-application data cards. The data card 10 is formed of plastic and contains solid state circuitry 12 having a microprocessor and memory chips. The memory chips hold the equivalent of several typewritten pages of information related to different applications. One application of the card is as a cash card with a stored cash value, thereby avoiding the need to purchase traveler's checks.

Thus, if Taylor teaches anything at all, it is merely a single credit/debit card that can be used for multiple accounts. There is no disclosure, teaching or suggestion in Taylor of "receiving at a metering device a request for a cryptographic certificate . . . determining if sufficient funds are present in the register for obtaining the certificate, if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key; sending a certificate request to a certificate authority, the certificate request including the public key of the cryptographic key pair; receiving a cryptographic certificate from the certificate authority, the cryptographic certificate including the public key of the cryptographic key pair generated by the metering device; deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair" as is recited in claim 35.

There is no disclosure in Fisher or Taylor, either alone or in combination, of "receiving at a metering device a request for a cryptographic certificate, the metering device including a register having funds stored therein . . . determining if sufficient funds are present in the register for obtaining the certificate, if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key; sending a certificate request to a certificate authority, the certificate request including the public key of the cryptographic key pair; receiving a cryptographic certificate from the certificate authority, the cryptographic certificate including the public key of the cryptographic key pair generated by the metering device; deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair" as is recited in claim 35.

The Office Action contends that it would have been obvious to combine the teachings of Fisher and Taylor to allow a user to protect user financial information while making a purchase over an insecure network. The Office Action has not provided any indication as to where such a suggestion is provided in the prior art. The fact that the present invention was made by the Applicant does not make the present invention obvious; that suggestion or teaching must come from the prior art. See C.R. Bard, Inc. v. M3 Systems, Inc., 157 F.3d 1340, 1352 (Fed. Cir.

1998). See, e.g., Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 1051-1052 (Fed. Cir. 1988) (it is impermissible to reconstruct the claimed invention from selected pieces of prior art absent some suggestion, teaching, or motivation in the prior art to do so.)

Even if, for arguments sake, one was motivated to combine the teachings of Fisher and Taylor, it still does not arrive at the present invention. There is no disclosure, teaching or suggestion in either of the references, either alone or in combination, of "determining if sufficient funds are present in the register for obtaining the certificate, if sufficient funds are present in the register, generating, at the metering device, a cryptographic key pair including a private key and a public key; sending a certificate request to a certificate authority, the certificate request including the public key of the cryptographic key pair; receiving a cryptographic certificate from the certificate authority, the cryptographic certificate including the public key of the cryptographic key pair generated by the metering device; deducting funds from the register for obtaining the requested certificate; and in response to funds being deducted from the register, activating the private key of the cryptographic key pair" as is recited in claim 35. As noted above, in Fisher the cryptographic key pair are generated and activated at the same time. This is not the same as in the present invention, in which the key pair is generated and the private key activated at different times. Without using the present claims as a road map, it would not have been obvious to make the multiple, selective modifications needed to arrive at the claimed invention from these references. The rejection uses impermissible hindsight to reconstruct the present invention from this reference. See Ex parte Clapp, 227 U.S.P.Q. 972,973 (Bd. App. 1985) (requiring "convincing line of reasoning" to support and obviousness determination).

For at least the above reasons, Applicants respectfully submit that claim 35 is allowable over the prior art of record. Claim 37, dependent upon claim 35, is allowable along with claim 35 and on its own merits.

In view of the foregoing remarks, it is respectfully submitted that the pending claims are in a condition for allowance and favorable action thereon is requested.

Respectfully submitted,

Brian A. Lemm
Reg. No. 43,748
Attorney for Applicants
Telephone No.: (203) 924-3836

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000